Voorkomen van fraude

Martin Scharenborg

Dit boek maakt deel uit van de Serie fraude en integriteit:

1. Uitkeringsfraude (ISBN 9789463185011)
2. Faillissementsfraude (ISBN 9789463185073)
3. Onderzoeken van fraude (ISBN 9789463185141)
4. Voorkomen van fraude (ISBN 9789463185172)
5. Fraude door werknemers (ISBN 9789463185240)
6. Fraude door ambtenaren (ISBN 9789463185271)
7. Fraude en accountant (ISBN 9789463185325)
8. Fraude in het strafrecht (ISBN 9789463185301)

Van dezelfde schrijver verschenen, de Serie tuchtrecht:

1. Tuchtrecht voor accountants (ISBN 9789463185905)
2. Tuchtrecht voor gerechtsdeurwaarders (ISBN 9789463185929)
3. Tuchtrecht voor advocaten (ISBN 9789463185943)
4. Tuchtrecht voor notarissen (ISBN 9789463185882)

Schrijver: M. Scharenborg
Coverontwerp: Sdu/Scharenborg
ISBN: 9789463185240

Voorwoord

Tien jaar geleden heb ik de serie fraude en integriteit geschreven. Door het verstrijken van de tijd en het opdoen van nieuwe kennis en ervaring werd het tijd voor het bijwerken van deze reeks en deze aanvullen met enkele nieuwe titels.

Het boek Voorkomen van fraude is een handreiking voor wie meer wil weten over het voorkomen van fraude en misbruik. Dit betekent dat ingegaan wordt op maatregelen gericht op personen, maar omdat voorkomen beter dan genezen is, worden ook maatregelen voor de organisatie uitgewerkt.
Een voorbehoud moet gemaakt worden met betrekking tot de uitdieping van de onderwerpen. Tal van onderwerpen in dit handboek rechtvaardigen een eigen boek. Dit handboek probeert het onderwerp fraude zo breed mogelijk te behandelen, maar niet elk onderwerp zal even uitgebreid aan bod komen.
Een tweede voorbehoud wordt gemaakt met betrekking tot het onderwerp *corporate governance*. Het handboek richt zich op fraude en misbruik, hetzij door de werknemer (intern), hetzij door een buitenstaander (extern). Het handboek richt zich niet op bedrijfsbeleid, waar *corporate governance* zich wel op richt. Dit onderwerp is dan ook niet nader uitgewerkt in dit handboek.
Een derde voorbehoud richt zich op hetgeen de organisatie kan doen als sprake is van fraude of misbruik. Dit is beschreven in het boek Onderzoeken van fraude, uit dezelfde serie.

Voor wat betreft de bronnen in dit boek merk ik op dat ervoor gekozen is om regelgeving en jurisprudentie zo veel mogelijk zakelijk weer te geven, hetgeen betekent dat zelden letterlijk geciteerd is, hoewel de afwijkingen niet groot zijn. Het voordeel hiervan is dat de tekst in dezelfde taalstijl is geschreven. Het nadeel is dat de tekst niet een (geheel) letterlijke weergave is. Als een lezer dus stuit op een relevante passage, dan doet hij er verstandig aan om de originele bron in de voetnoot te raadplegen.

Martin Scharenborg, 2016

Inhoudsopgave

Hoofdstuk 1 Algemeen

1.1 De fraudeur

1.1.1 Cijfers[1]

Uit cijfers van het Centraal Bureau voor de Statistiek (CBS) blijkt dat in 2014 er 1.006.770 delicten zijn gepleegd, onder te verdelen in:

- 623.960 vermogensmisdrijven (opgelost 14%);
- 134.370 vernielingen (opgelost 19%);
- 97.020 geweld- en seksuele misdrijven (opgelost 64%);
- 114.470 verkeersmisdrijven (opgelost 37%);
- 15.850 drugsmisdrijven (opgelost 92%);
- 5.860 wapenmisdrijven (opgelost 94%).

De grootste categorie, de vermogensmisdrijven, kan als volgt onderverdeeld worden:

- 587.050 diefstallen of verduisteringen en inbraken;
- 10.330 diefstallen en inbraken met geweld;
- 576.720 diefstallen en inbraken zonder geweld;
- 18.780 bedrogmisdrijven;
- 9.130 valsheidsmisdrijven;
- 6.790 helingen;
- 1.450 afpersingen en afdreigingen;
- 770 overige vermogensmisdrijven.

NB Opgemerkt moet worden dat computervredebreuk opgenomen is onder de categorie vernielingen. In 2014 waren dit er 1.990. Dit delict wordt ook vaak gepleegd ten behoeve van het verkrijgen van geld en kan dus onder omstandigheden gezien worden als fraude (het middel om fraude te plegen).

De meest gepleegde misdrijven hebben het laagste oplossingspercentage. Nu wordt nagenoeg het gehele component vermogensmisdrijven gevormd door diefstallen en heling. Bedrog en valsheid in geschrifte, typische fraudedelicten, vormt tezamen ruim 4% van de vermogensmisdrijven.
Het lage oplossingspercentage is helaas niet bekend voor de onderverdeling in delicten. Dat vermogensmisdrijven niet een hoog oplossingspercentage hebben is niet vreemd:

- De crimineel denkt na voordat hij steelt, liegt of bedriegt (geweld geschied in emotie). Een geldgedreven delict heeft een anders handelende verdachte dan een emotiegedreven verdachte (zoals bij moord, verkrach-

[1] Cijfers CBS, rapport Criminaliteit en rechtshandhaving 2014

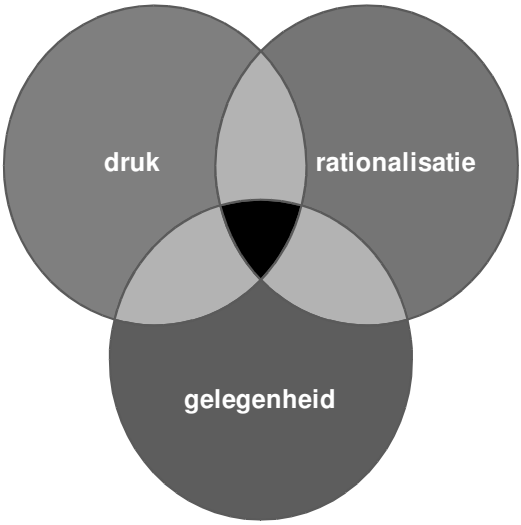
ting of mishandeling). Sporen worden daar nagelaten die door de dna databank gehaald kan worden. Bij fraude is het allemaal complexer.
- De crimineel doet dit niet zelden bij vreemden, zodat er geen link is tussen beiden.
- De aantallen zijn zo hoog dat er niet voldoende opsporingscapaciteit is om alles tot in de puntjes te rechercheren (hetgeen bij moord en verkrachting wel moet gebeuren).

1.1.2 De fraudefactoren

Waarom frauderen niet veel meer mensen? Waarom neemt niet iedere werknemer geld uit de kassa van zijn werkgever weg, of neemt hij goederen zonder te betalen mee naar huis? Veel werknemers hoeven hier weinig moeite voor te doen, kansen te over.
Een deel van de reden is de risico-analyse die een fraudeur maakt (zie hierna). Maar dan is de overweging om te frauderen al gemaakt, de werknemer is al verworden tot potentiële fraudeur. Maar hoe wordt een werknemer een potentiële fraudeur?

Een werknemer verwordt tot potentiële fraudeur als er sprake is van gelegenheid om te frauderen, de druk er is te frauderen en een te plegen fraude gerationaliseerd wordt.

Dit kan als volgt weergegeven worden:



Daar waar in het venndiagram de cirkels samenkomen, daar is een potentiële fraudeur 'geboren'. Een nadere toelichting op de factoren is vereist.

De factor gelegenheid zorgt ervoor dat er gefraudeerd kan worden. Gelegenheid is er bijvoorbeeld als de werkgever de sleutel van de kluis in een open lade bewaart, of als de werknemer onbeperkt toegang tot de bankrekeningen heeft en daardoor in staat is geld over te boeken naar de eigen bankrekening.
De factor rationalisatie zorgt ervoor dat het geweten van de persoon uitgeschakeld wordt, tenminste dat het verrichten van niet-integere handelingen gerationaliseerd wordt (gerechtvaardigd). Een ieder weet dat het toe-eigenen van geld van anderen niet hoort. Deze barrière zorgt ervoor dat relatief weinig fraude wordt gepleegd. Immers veel werknemers kennen de zwakke plekken in de organisatie, maar gebruiken deze kennis doorgaans niet ten eigen bate. Hun moreel-ethisch besef houdt hen tegen.
De factor druk zorgt voor de noodzaak voor het plegen van fraude. De prikkels die leiden tot het ervaren van druk kunnen persoonlijk of zakelijk van aard zijn. Bij persoonlijke prikkels kan gedacht worden aan geldproblemen door verslaving (gokken, drugs), problemen in de relationele sfeer (echtscheiding), financiële problemen bij de partner (slecht lopend bedrijf), maar ook een bovenmatig uitgavenpatroon. Zakelijke prikkels zijn de *targets* die de werknemer niet gehaald heeft waardoor hij een bonus of promotie misloopt, of een te lage beurskoers waardoor toegekende opties waardeloos zijn geworden. Deze financiële prikkels kunnen de werknemer motiveren om fraude te plegen, bijvoorbeeld door het 'oppompen' van resultaten. Hoe groot de gevolgen hiervan kunnen zijn maken fraudezaken als Enron en Ahold wel duidelijk.
De factoren zijn als gelijkwaardige cirkels weergegeven. Dit betekent niet dat elke factor in gelijke mate aanwezig is. Ieder persoon heeft hier een eigen invulling bij, de een heeft een sterk, de ander een beperkt geweten. Zo kan ook de een veel financiële problemen hebben en de ander weinig. Met andere woorden, elk individu zal een grootte van cirkels hebben die past bij zijn eigen situatie, zodat deze groter of kleiner kunnen zijn al naar gelang de situatie van die persoon op dat betreffende moment.
Daar waar twee cirkels elkaar snijden ontstaan grijze gebieden. Hier is nog geen sprake van fraude, maar de kans dat de werknemer in de verleiding komt om te frauderen neemt toe. Hij kan dan wel erg snel kan besluiten dat de derde factor is vervuld, waardoor hij in het zwarte veld belandt. Dit komt omdat zowel de factor druk als rationalisatie zich met name in het hoofd van de potentiële fraudeur afspelen. Zodra er gelegenheid is (zoals een open kluis met veel contant geld), dan is het louter het innerlijke proces dat besluit of er wel of niet gefraudeerd wordt. Als de druk er dan ook is, dan kan de druk te groot worden. De werknemer moet dan een sterk geweten hebben om niet het frauderen te gaan rationaliseren. Heeft de werkgever hem voor een promotie overgeslagen, dan kan uit wrok de fraude al snel voor hemzelf gerechtvaardigd zijn.
De knop in het hoofd van de werknemer kan ook omgezet worden als er gelegenheid en rationalisatie is, alleen nog geen druk. De werknemer hoeft dan alleen op zoek naar een reden, meestal van financiële aard. Komen de

dure feestdagen er weer aan, moet de belasting weer betaald worden, wilde de werknemer nu een keer ver weg met vakantie? Als twee van de drie factoren aanwezig zijn, dat kan de potentiële fraudeur druk voelen om de derde factor te vervullen.
De drie-eenheid van fraude verklaart waarom het die collega's zijn die frauderen waar niemand het van had verwacht: de boekhouder die al twintig jaar werkt bij de bank en dan ineens fictieve cliënten gaat opvoeren om zo via fictieve leningen geld van de bank te kunnen ontvreemden. De onderzoeker hoort dan vaak verbaasde reacties van collega-werknemers en managers dat de werknemer juist zo betrouwbaar was, hart voor de zaak had en altijd hard werkte. Dat klopte tot het moment voor de fraude ook. In al die jaren was nog geen sprake van vervulling van alledrie de voorwaarden. Bij het plegen van de fraude was daarvan wel sprake. Een dergelijk plotselinge omschakeling wordt meestal door de factor druk of rationalisatie veroorzaakt. Gelegenheid is vaak al bekend bij de werknemer. Rationalisatie en druk zijn dan de nog de knoppen in het hoofd die om moeten.

1.1.3 Kosten-batenanalyse

Wat maakt een potentiële fraudeur tot een fraudeur? De risico-analyse.

Hoe vreemd het mogelijk ook klinkt, fraude is een zaak van kosten-baten-analyse, zowel voor de fraudeur als voor de benadeelde organisatie.
De fraudeur weegt de mogelijke opbrengst van de fraude af tegen de kosten die met de fraude gepaard gaan en de kans om gepakt te worden.
De organisatie weegt de kans op fraude af tegen de kosten van het nemen van maatregelen om fraude te voorkomen.
Hoewel het uitgangspunt van fraudeur en benadeelde organisatie verschillen is het uitgangspunt hetzelfde, beiden maken een afweging van de kosten.

De rechtseconomie leert ons dat de crimineel (en dat is ook de fraudeur) een afweging maakt, namelijk de zwaarte van de straf en de pakkans versus de verwachtingswaarde van het strafbaar handelen.
Nentjes stelt dat de nutsmaximaliserende crimineel, de *homo economicus criminalis*, een keuzeprobleem heeft: gaat hij strafbare feiten plegen en zo ja, in welke mate? Hij stelt dat de crimineel een zodanig criminaliteitsniveau kiest dat het maximale nettobaten oplevert.[2]

In de economie wordt de risico-analyse als volgt weergegeven:

kans x gevolg < voordeel

De kans is in dit geval de pakkans. Voor fraude is dit niet erg hoog, veertien procent. Het gevolg dat men vreest voor het moeten zitten in de cel mag dan

[2] A. Nentjes, Elementaire rechtseconomie, Wolters-Noordhof, Groningen 1995.

beperkt zijn, er zijn ook andere gevolgen, zoals het betalen van schadevergoeding, het ontslagen worden en gezichtsverlies bij vrienden en familie. Die factoren spelen een belangrijke rol om niet te verworden tot crimineel, ook al is de potentie er.

Pakkans en het gevolg worden afgezet tegen het voordeel van de fraude. Als deze lager is dan het voordeel, dan wordt de potentiële fraudeur een fraudeur.

1.2 De organisatie

1.2.1 Schade

De meest duidelijke schade voor de organisatie in geval van fraude is wat de fraudeur ontvreemdt: de waarde van de goederen of het geld. Maar er is meer schade.
Als eerste kan gewezen worden op de schade die veroorzaakt is door het ontvreemden van het goed of de goederen. De kosten van een gebroken raam, slot, deur, het kapotmaken van het alarmsysteem, maar ook de kosten van het herprogrammeren van het computersysteem.
Als tweede kan gedacht worden aan de uren die door de werknemers in de organisatie besteed moeten worden aan de fraude, zoals het herstellen van de schade, voor zover mogelijk, het overleg over de fraude, wat er aan te doen en dergelijke. Gezien het belang betreft dit niet alleen urenverlies van de collega's van de fraudeur (in geval van interne fraude), maar ook die van de directie, hoofd personeelszaken en hoofd juridische zaken.
Als derde kan gedacht worden aan de deskundigen die ingehuurd worden. Dit kan een advocaat zijn, maar ook een particulier onderzoeker of een forensisch accountant.
Als vierde kan gedacht worden aan de kosten voor ontslag en aantrekken van een nieuwe werknemer in geval van interne fraude. Dit betekent juridische kosten (advocaat, griffie), maar ook personeelskosten zoals het plaatsen van advertenties, het testen van de sollicitanten en het productieverlies van het inwerken van de nieuwe werknemer.
Als vijfde kan gedacht worden aan de kosten voor het updaten van het beveiligingsbeleid van de organisatie naar aanleiding van de fraude. Niet alleen moet voorkomen worden dat de fraude opnieuw kan plaatsvinden, ook moet de organisatie gescreend worden op andere zwakheden, om te voorkomen dat andere potentiële fraudeurs 'bloed ruiken'.
Als zesde kan gedacht worden aan reputatieschade, wat mogelijk kan leiden tot verlies van klanten. Immers als de klanten erachter komen dat de organisatie kwetsbaar is voor fraude, hoe veilig is het dan om zaken met hun te doen?
Als zevende kan gedacht worden aan de kosten van stijging van de verzekeringspremie. Als de verzekeraar heeft moeten uitkeren zal deze nagaan of de verzekerde voldoende maatregelen tegen fraude heeft genomen

en zonodig aanvullende maatregelen eisen. Sowieso kan door de uitkering de verzekeringspremie stijgen.

De organisatie kan slechts een klein deel van de kosten op de fraudeur verhalen, zoals de waarde van hetgeen ontvreemd is, de direct daardoor ontstane schade en mogelijk de onderzoekskosten die daarop volgen. Het is aan de rechter om te bepalen in hoeverre toerekening redelijk is.
Hoewel de benadeelde organisatie de schadevordering (in theorie) kan voegen in een strafproces, zal de strafrechter in de praktijk de schadevordering niet zelden afwijzen als zijnde te complex en verwijzen naar de civiele rechter voor afhandeling. De benadeelde organisatie moet dan zelf naar de civiele rechter om de schade te verhalen op de fraudeur.
De vraag in de praktijk is of de fraudeur over voldoende vermogen beschikt om de schade te kunnen betalen. Hij fraudeerde immers niet omdat hij veel geld heeft: geldnood is niet zelden de reden om te gaan frauderen.

1.1.1 Preventieve maatregelen

Wil de organisatie een potentiële fraudeur niet laten verworden tot een voltooide fraudeur, dan dienen maatregelen genomen te worden die de facturen van fraude beïnvloeden. Hoe die maatregelen opgesteld kunnen worden komt verder in dit boek aan de orde, hier wordt volstaan met een opsomming per fraudefactor.

Factor gelegenheid
Van de drie factoren die nodig zijn om tot fraude te komen is gelegenheid de factor waar de organisatie het meeste invloed op kan uitoefenen. Het is voor een organisatie relatief eenvoudig, zij het soms duur, om maatregelen te treffen die de gelegenheid beperken of zelfs uitsluiten. Hierbij moet niet alleen naar de kosten van de maatregel gekeken worden, maar ook naar de haalbaarheid. Zo is de beste manier om te voorkomen dat geld gestolen wordt het op te bergen in een zware kluis. Echter het doel van geld is nu juist dat er betalingen mee verricht kunnen worden. Dit betekent dat niet voor absolute beveiliging (voor zover dat al mogelijk zou zijn) gekozen kan worden, maar voor een haalbare beveiliging, waarbij het gebruik in de praktijk moet worden afgewogen tegen het risico op misbruik.

Bij te treffen maatregelen kan gedacht worden aan:
- Het beveiligen van het geld (kluizen, kasregistratie).
- Het beveiligen van de goederen (registratie, camera's).
- De beveiliging van het computernetwerk (wachtwoorden, encryptie, firewall, virusscanners).
- De beveiliging van de gebouwen (toegangscontrole, hang- en sluitwerk, camera's, kluizen).
- Functieroulatie om belangenverstrengeling te voorkomen.
- Functiescheiding om tegengestelde belangen te creëren.

- Informatiebeveiliging.
- De registratie van de locatie van waardevolle objecten (tracking).
- Het screenen van nieuw en huidig personeel.
- Het tegengaan van solistische (en dus ongecontroleerde) functieuitoefening door werknemers.
- Verantwoording van de gewerkte uren.
- Het verzekeren van waardevolle objecten.
- Vier ogentoezicht bij het tellen van geld of voorraad.

Het invoeren van de maatregelen betekent niet dat fraude niet meer kan voorkomen: de fraudeur kent de organisatie door en door en kan door de jarenlange ervaring gaten in de maatregelen ontdekken. De organisatie mag dan ook niet te veel vertrouwen op getroffen maatregelen en dient zich te richten op het beperken van de factoren druk en rationalisatie.
Echter druk en rationalisatie kunnen, voor zover deze al te beïnvloeden zijn, alleen gericht zijn op de werknemer. De fraudeur kan ook een buitenstaander zijn. Het is dan ook van belang dat er wel degelijk veel aandacht wordt besteed aan het treffen van maatregelen, omdat deze personen via de andere factoren niet of moeilijk zijn te beïnvloeden.

Factor rationalisatie
De factor rationalisatie heeft betrekking op de persoon. Het is de natuurlijke weerstand die een persoon heeft om niet te frauderen of om niet-integere handelingen te verrichten. Deze factor kan in beperkte mate beïnvloed worden zodat gepoogd kan worden om de interne fraude te beperken.
De uitgewerkte maatregelen gelden alleen voor werknemers. Externe fraudeurs worden hier niet mee bereikt. Beïnvloeding van derden kan wel, maar is kostbaar en het effect is beperkt. Denk bijvoorbeeld aan ideële reclame, zoals de advertenties van de Bond tegen Vloeken die via ludieke reclameacties mensen probeert te overtuigen dat het niet juist is om de naam van God te misbruiken. Op het gebied van fraudebestrijding zenden platenmaatschappijen spotjes uit waarin wordt getoond dat het downloaden van muziek of films hetzelfde is als het stelen van producten uit de winkel. In beide gevallen proberen derden een persoon te beïnvloeden en aan te geven wat goed en slecht is. Ze proberen op te voeden. De opvoeding is ook de plek waar het geweten, de normen en waarden, gevormd worden. Dit volgt uit het handelen van de ouders (voorbeeldgedrag), het handelen van de groep waarin de persoon optreedt (*peer pressure*) en het handelen van de persoon zelf (het geweten).
Gelet op voorgaande zal het beïnvloeden van onbekenden geen optie zijn voor de meeste organisaties die zich tegen fraude willen verweren. De organisaties zullen zich dan ook met name richten op de eigen werknemers, om zo de interne fraude pogen te voorkomen, dan wel te verminderen.

Bij te treffen maatregelen kan gedacht worden aan:
- Het afleggen van de eed of belofte (overheid).
- Het gebruikmaken van heldere declaratieprocedures.
- Het tonen van duidelijkheid, openheid en consistentie in gedrag.
- Heldere functiebeschrijvingen waaruit blijkt wat van werknemers wordt verwacht.
- Het geven van dilemmatrainingen.
- Het houden van functioneringsgesprekken.
- Het gebruikmaken van offerteprocedures en aanbestedingsbeleid.
- Het opstellen en invoeren van gedragscodes.
- Het opstellen en invoeren van protocollen (kas, inventarisatie).
- Het tonen van voorbeeldgedrag door de leiding (*tone at the top*).

Via procedures, codes, richtlijnen, trainingen en gesprekken wordt de werknemer duidelijk gemaakt wat wel en niet kan. Er wordt een verwachtingspatroon geschapen. Hierdoor wordt het de werknemer duidelijk of zijn moraal overeenstemt met die van de organisatie en of zijn handelen acceptabel is. Kennis hiervan zorgt ervoor dat, als de werknemer voor de keuze komt om te frauderen, hij weet hoe er binnen de organisatie over gedacht wordt en dat zij dit handelen als fout aanmerkt. Het is dan ook aan de werknemer om weerstand te bieden tegen de verleiding.
Overigens kan niet genoeg benadrukt worden dat de rol van het management van grote invloed is. Als de directeur zich niet houdt aan de gedragscode, dan zal de werknemer zich er ook niet veel gelegen aan laten. Hierbij moet rekening gehouden worden dat dergelijk gedrag van de leiding populaire koffiepraat is en snel de organisatie zal doorgaan. Denk aan maar de term Maseratiman, de frauderende ex-bestuurder van de Amsterdamse woningcorporatie Rochdale.[3]

> Zo was er een leidinggevende die op een door de organisatie verstrekte laptop in zijn privéomgeving, maar op de zakelijke computer en dus via het zakelijke netwerk, pornosites bezocht, hetgeen volgens de gedragscode niet was toegestaan. Op enig moment liep de laptop vast en schakelde de leidinggevende de IT-afdeling van de organisatie in. Deze stelden al snel vast dat er sprake was van een virus, opgelopen door het surfen naar pornosites. Enige dagen later was het een publiek geheim in de organisatie wat de leidinggevende had gedaan. De geloofwaardigheid van de leidinggevende is dan verdwenen door het negatieve voorbeeldgedrag.

Factor druk
De factor druk is het moeilijkst te bestrijden, omdat dit veelal in de privésfeer plaatsvindt. Het ervaren van druk om te frauderen kan zijn ingegeven door geldproblemen veroorzaakt door een verslaving, een echtscheiding, maar ook een te hoog uitgavenpatroon. Deze factor kan door goed personeelsbeleid onderkend worden en zo mogelijk ondervangen worden. Zo kan een collega die verslaafd is opgevangen worden en via de bedrijfsarts in een opvang-

[3] www.volkskrant.nl/binnenland/rechter-veroordeelt-maserati-man-tot-2-5-jaar-cel~a4205157/

traject geplaatst worden voordat de verslaving uit de hand loopt en de gevolgen op de werkvloer merkbaar worden. Het voordeel hierbij is niet alleen dat de kans op fraude verkleind wordt, maar ook dat de werknemer door de werkgever opgevangen wordt in moeilijke tijden, hetgeen de betrokkenheid van veel meer werknemers zal vergroten. De werkgever gaat voor hen net een stapje verder. Hiertegenover staat wel dat de werkgever zich actief gaat bemoeien met iets wat de meesten beschouwen als privé, zodat de grens tussen privé en zakelijk overschreden wordt. De vraag is of men dit wel wil en of dit wel kan. Voorzichtigheid is hierbij dan ook troef, waarbij de bedrijfsarts of vertrouwenspersoon een belangrijke rol kan vervullen.
In plaats van een persoonlijke benadering kan de organisatie ook kiezen voor een zakelijke benadering. De prikkel om te frauderen is bijna altijd financieel ingegeven. Het verstrekken van een substantiële loonsverhoging aan degene die geldelijke problemen heeft kan de druk om te frauderen wegnemen. Dergelijk beleid levert echter tal van nieuwe problemen op. Het is niet altijd duidelijk wie dermate lijdt onder financiële problemen dat deze fraude overweegt. Het aan een ieder met geldproblemen verstrekken van salarisverhoging is geen optie. Zelfs al zou de mogelijke fraudeur onderkend kunnen worden en zou de loonsverhoging economisch bezien goedkoper zijn dan de schade van de fraude (waaronder ook het ontslagtraject), dan nog is loonsverhoging voor iemand die zou kunnen frauderen niet te rechtvaardigen. Dergelijke acties hebben bij de overige medewerkers tot gevolg dat de loyaliteit afneemt, zodat het gevaar bestaat dat de factor rationalisatie sneller bij hun vervuld zal zijn. Immers zij zien dat hard werken niet leidt tot salarisverhoging, maar het willen plegen van criminele activiteiten daar wel toe leidt. Deze onrechtvaardige (maar vanuit rechtseconomie begrijpelijke) behandeling zal een scala aan nieuwe potentiële fraudeurs kunnen opleveren.

Vormen van druk waar de organisatie zelf verantwoordelijk voor is:
- Het koppelen van bonussen aan hoge *targets.*
- Promotie koppelen aan omzetstijging.
- Het uitbetalen van loon in een vast en een variabel deel.
- Het verstrekken van opties, zodat de hoogte van het salaris afhankelijk is van de koersontwikkeling.

1.2.2 Risico-analyse

De organisatie kan via risico-analyse bepalen of het treffen van maatregelen haalbaar is. De risico-analyse omvat de volgende afweging: kosten van de maatregelen x de kans op fraude is kleiner dan de kosten van schade door de fraude.
Om deze analyse mogelijk te maken moet de organisatie de volgende fasen doorlopen:[4]
- Het in kaart brengen van objecten/activiteiten die risico lopen.

[4] www.en.wikipedia.org/wiki/Vulnerability_assessment

- Het toekennen van een waarde aan het object/activiteit.
- Het identificeren van kwetsbaarheden of potentiële bedreigingen aan het object/activiteit.

Als vervolgens de risico's geïdentificeerd zijn, dan zijn de volgende oplossingen mogelijk:
- Risicovermijding, door het proces of de activiteit niet uit te voeren (geen contant geld bewaren in de organisatie).
- Risicobeperking, door het treffen van maatregelen die de schade moeten beperken (zoals het plaatsen van een sprinklerinstallatie tegen het risico van brand).
- Risico-acceptatie, dit vindt plaats als de kosten van het treffen van maatregelen groter is dan de kosten van het risico.
- Risico-overdracht, het risico verplaatsen naar een ander, bijvoorbeeld door zich te verzekeren voor de gevolgen van fraude.

Het proces van risico-analyse dient gestructureerd plaats te vinden op basis van risicomanagement. Dat kan betekenen het (tijdelijk) aantrekken van een risicomanager die de risico's en de daarvoor te nemen maatregelen in kaart brengt en vastlegt. In een risicoplan wordt voor elk risico bepaald welke oplossing de beste is voor de organisatie.
Zowel de risico-analyse als het risicoplan wordt periodiek bijgewerkt. Dit is niet alleen noodzakelijk om vast te stellen of de maatregelen die voorheen gekozen waren nog steeds effectief zijn, maar ook om vast te stellen of de risico's niet zijn veranderd. Zo kunnen er nieuwe beveiligingsmogelijkheden zijn (nieuwe maatregelen), maar kunnen er ook nieuwe technieken zijn om processen te manipuleren (nieuwe risico's). Vooral met betrekking tot de informatietechnologie geldt dat de ontwikkeling een continu proces is.[5]

1.3 Wat te doen bij fraude?

1.3.1 Stappenplan

Wat kan de organisatie doen als de fraude gepleegd en ontdekt is? Om nit voor een volslagen verrassing te komen te staan, is het verstandig dat er een draaiboek fraude is, net zoals er een draaiboek is voor andere onvoorziene gebeurtenissen (brand, bommelding). Een goed draaiboek zorgt ervoor dat in het begin geen fouten gemaakt worden die de organisatie later kunnen opbreken. Zo is het niet ongebruikelijk dat een organisatie bij fraude schrikt en overhaast maatregelen neemt. Niet zelden legt de rechter de gevolgen daarvan bij de werkgever, hetgeen leidt tot schadevergoeding bij ontslag voor de werknemer, soms zelfs als de werknemer in kwestie schuldig is.[6]

[5] www.en.wikipedia.org/wiki/Risk_Management

[6] De schuldvraag blijkt in sommige gevallen van ondergeschikt belang te zijn als de organisatie procedurele regels en rechtsbeginselen geschonden heeft. Vooral in het arbeidsrecht kan dit leiden tot

Een draaiboek voor fraude zou kunnen bestaan uit de volgende stappen:

1. Het samenstellen van een projectgroep met daarin de directeur, het hoofd personeelszaken en een jurist.
2. Het aanstellen van een contactpersoon.
3. Het bijhouden van een logboek.
4. Het inschakelen van externe deskundigen (advocaat, onderzoeker).
5. Het afsluiten van de fysieke en elektronische toegang.
6. Het controleren van het het geld, de goederen.
7. Het controleren van de verzekeringspolis (vanwege de maatregelen die genomen moeten wil er dekking zijn).
8. Het overwegen van het treffen van (orde)maatregelen tegen de betrokkene.
9. Het opleggen van een mediaverbod aan de medewerkers.
10. Het waarschuwen van de accountant.

Een toelichting per stap.

1. Binnen de organisatie moet voor incidenten een projectgroep worden opgericht voor het begeleiden van de afhandeling van een (omvangrijke) fraude. De samenstelling van het projectteam bestaat uit vaste en wisselende leden. De vaste leden zijn een lid van het bestuur, het hoofd personeelszaken en de bedrijfsjurist. De wisselende leden worden ingeschakeld naarmate hun deskundigheid nodig is voor de incidentbegeleiding, zoals een medewerker van de afdeling Integriteit zijn in geval van fraude.
2. De projectgroep stelt een contactpersoon. De taak van de contactpersoon is het aansturen van het onderzoek, het faciliteren van de onderzoekers en het voorzien van de projectgroep van informatie.
3. De contactpersoon houdt een logboek bij waarin hij vastlegt welke afspraken hij maakt, met wie hij spreekt, wat voorgevallen is. Kortom, de zeven w's (wie, wat, waar, wanneer, waarom, waardoor en welke). Hierdoor kan achteraf vastgesteld worden wat er is gebeurd en hoe er is gehandeld. Het logboek voorkomt dat achteraf onduidelijk is wat er is gebeurd en waarom.
4. De projectgroep kan de contactpersoon opdracht geven een advocaat in te schakelen die de juridische situatie kan inschatten. De advocaat kan ook inschatten of aanvullend bewijs nodig is, zodat een particulier onderzoeker ingeschakeld dient te worden. Ook kan gedacht worden aan het inschakelen van een woordvoerder. De woordvoerder kan aangeven hoe het beste met de fraude omgegaan kan worden. Zo kan het zinvol zijn om een deel van de gebeurtenissen in de organisatie bekend te maken, om zodoende de werknemers duidelijk te maken wat er aan de hand is en waarom maatregelen getroffen zijn zoals schorsing. Vaak is er een borrelpraatcircuit die bij incidenten een eigen leven gaat leiden en waarbij al snel de zaken gepolariseerd worden (leiding versus werk-

ontbinding van de arbeidsovereenkomst, waarbij het de werkgever is die (soms forse) compensatie moet betalen aan de werknemer.

nemers). Hierbij moet natuurlijk wel de privacy in acht genomen worden van de betrokkenen, alsook de onderzoekstactische overwegingen.

5. Als de fraudeur doorheeft dat hij ontdekt is, of de organisatie niet het risico kan lopen dat hij doorgaat, dan moeten onmiddellijk ordemaatregelen getroffen worden. Dit kan bijvoorbeeld schorsing van de werknemer in het belang van het onderzoek zijn (na raadpleging van een advocaat), het innemen van de laptop en de sleutels van de werknemer, alsook het veranderen van de toegangscodes tot het netwerk. Via onderzoek van de werkplek kunnen informatiebronnen als computer en de zakelijke agenda veiliggesteld worden.
6. De kassier en magazijnmeester dienen met een leidinggevende direct de aanwezige voorraden te controleren, zoals ook het hoofd administratie met de contactpersoon direct de saldi van de bankrekeningen controleert.
7. De verzekeringspolissen worden doorgenomen om vast te stellen of de fraude gedekt wordt. Indien dat het geval is, dienen tijdig de polisvoorwaarden doorgenomen te worden om vast te stellen of hierin bijzondere voorwaarden staan waaraan de organisatie moet voldoen. Zo zou een voorwaarde kunnen zijn dat aangifte moet worden gedaan van de fraude. Het kan zijn dat de organisatie geen aangifte wil doen, bijvoorbeeld uit angst voor negatieve publicitaire gevolgen. In dat geval zal de organisatie geen claim bij de verzekeraar indienen. Dit moet dus tijdig duidelijk zijn.
8. Na afronding van het fraudeonderzoek moet de projectgroep de gevolgen van de fraude verwerken in het integriteitsbeleid. Dat betekent het aanpassen van de maatregelen van interne controle en administratieve organisatie (gericht op de factor gelegenheid), alsook de cultuur die de fraude mogelijk heeft gemaakt (gericht op de factor rationalisatie). Dat kan betekenen dat de gedragscode verbeterd moet worden, of meer training gegeven moet worden.
9. In overleg met de advocaat kan ook overwogen worden om na uitleg van de situatie een spreekverbod op te leggen.
10. De controlerend accountant dient geinformeerd te worden over de fraude. Dit heeft kan gevolgen hebben voor de controle en de accountantsverklaring.

1.3.2 Communicatiebeleid[7]

In het stappenplan is gewezen op het aanstellen van een woordvoerder, om zodoende zowel intern als extern op een correcte manier te kunnen communiceren over de integriteitsschending en de gevolgen die dat heeft gehad. Het Bureau Integriteitsbevordering Openbare Sector (BIOS) van het ministerie van Binnenlandse Zaken heeft veertien aanbevelingen met betrekking tot de communicatie over integriteitsschendingen uitgebracht:

[7]Deze paragraaf is afgeleid van de brochure Schandaal Management, Aanbevelingen met betrekking tot communicatie over integriteitsschendingen, november 2005, Bureau Integriteitsbevordering Openbare Sector (www.integriteitoverheid.nl).

- veronachtzaam de voorbereiding niet;
- geef bestuurders en ambtelijke managers een mediatraining;
- ontwikkel in rustiger tijden relaties met journalisten;
- interne en externe communicatie moeten in balans zijn;
- organiseer interdisciplinair overleg;
- geef de regie niet uit handen;
- neem zelf het initiatief in het communiceren met de pers;
- maar wees beducht voor te snelle communicatie;
- pas op voor meegaan in geruchten;
- respecteer de privacy van de betrokkene(n);
- rehabilitatie;
- durf impopulaire maatregelen te nemen;
- denk niet te snel in termen van incidenten;
- beperk contacten met ongenode gasten.

Voorbereiding
Het is van belang dat de organisatie niet afwacht totdat een incident zich voordoet voordat ze een plan opstelt hoe daarop gereageerd moet worden. Het vooraf opstellen van een communicatiebeleid inzake integriteitsschendingen heeft de volgende voordelen:
- De leidinggevenden en staffunctionarissen krijgen dezelfde focus.
- Het beleid maakt duidelijk wie wanneer reageert, waardoor tegenstrijdige en imagobeschadigende reacties voorkomen kunnen worden.
- Het beleid zorgt ervoor dat alle mogelijke doelgroepen tijdig onderkend zijn, zodat in de hectiek van het incident geen partijen worden vergeten.
- Het beleid maakt duidelijk wie op de hoogte gesteld moet worden.
- Het beleid maakt het mogelijk op mensen bij te sturen die niet goed hebben geopereerd in de media.
- In het beleid is aandacht aan het blijven onderhouden van contact tussen organisatie en betrokkene, zodat onnodige verharding van standpunten kan worden vermeden.

Mediatraining
Door middel van mediatraining kan voorkomen worden dat de organisatie onnodig schade leidt bij het communiceren over het incident. Zo kan een leidinggevende verleid worden meer te vertellen dan verstandig is en waarna uitspraken door de betrokkene in juridische procedures gebruikt worden. De mediatraining is gericht op het oefenen van interviews, het geven van een persconferentie en het beantwoorden van vragen.

Ontwikkeling relatie journalisten
Als een relatie met journalisten ontwikkeld wordt voordat sprake is van een incident, kan in tijden van een incident beter overlegd worden met de journalist. Men kent elkaar waardoor de journalist makkelijker kan worden